UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DIANNA LARSON, MATTHEW GATES, CHRISTY ADAMS and GARY MARES,	Case No.
Plaintiffs,	
v.	**CLASS ACTION COMPLAINT**
EQUIFAX, INC.,	**JURY TRIAL DEMANDED**
Defendant.	

Plaintiffs Dianna Larson, Matthew Gates, Christy Adams, and Gary Mares ("Plaintiffs"), individually, and on behalf of the Class defined below of similarly situated persons, file this Class Action Complaint, against Equifax, Inc. ("Equifax").

INTRODUCTION

1. From March through July of 2017, Equifax experienced one of the largest data security breaches in history (the "Data Breach"). Cyber attackers stole the personally identifiable information ("PII") of approximately 145 million Americans from Equifax's files. ("Class Members").

2. In the face of this extraordinary event which caused so much harm to so many innocent Americans, three key executives of Equifax decided that this was the time to extract an extraordinary profit based on their inside information, before

information about the breach became public. These executives dumped nearly $1.8 million in stock holdings shortly after July 29. On August 1, Chief Financial Officer John Gamble sold shares worth $946,374 and another executive, Joseph Loughran, exercised $584,099 in stock options. The following day, Rodolfo Ploder sold $250,458 in Equifax stock. Following Equifax's September 7 data-breach announcement, shares plummeted more than 13%, wiping out more than $2 billion in investors' assets.

3. Equifax is one of the three major consumer credit reporting agencies in the United. States. As such, it gathers sensitive financial data on consumers' payment history, then sells data to banks, insurance companies, potential employers, landlords, and government agencies in the form of a Consumer Credit Report ("Credit Report"). In other words, the victims of this data breach unlike so many others are not the company's customers; it is the innocent people whose data Equifax sold to its customers.

4. For millions of consumers, Credit Reports have become a ubiquitous element of everyday life. Whether applying for a credit card, a mortgage, a car loan, a job, or a residential lease, consumers, financial institutions, employers, and landlords rely upon Credit Reports. As a practical matter, it would be nearly

impossible for consumers to conduct business without their PII ending up in the possession of Equifax and other consumer credit agencies.

5. Numerous entities, including the IRS, rely upon Credit Report data to verify an individual's identity. For example, individuals may be asked to choose a street where they lived or the name of their student loan lender from a list. The ability to correctly answer these questions verifies an individual's identity. With access to Credit Report data, criminals can now correctly respond to these verification questions, a process known as "pretexting".[1]

6. This is the third data breach at Equifax since 2015. Despite two prior incidents and the fact that it was storing sensitive personal information that it knew was valuable to, and vulnerable to, cyberattackers, Equifax failed to take security precautions that could have protected Class Members' data. Instead, Equifax used grossly inadequate computer systems and data security practices that allowed the hackers to easily make off with Class Members' PII. For example, the Department of Homeland Security warned Equifax on March 8, 2017 about the need to patch a particular vulnerability in software Equifax used. The company emailed out that warning the following day and requested that applicable personnel install the

[1] Equifax itself uses this verification process as part of its TrustedID Premier signup process.

upgrade. While Equifax's policy required the upgrade to occur within 48 hours, that did not occur according to the Company's former CEO, Richard Smith.

7. The Equifax database included the types of information that federal and state law requires companies to take security measures to protect: names, dates of birth, Social Security numbers, driver's license numbers, employment information, and credit card numbers. These data should have received extra protection, not substandard protection.

8. Defendant made repeated promises and representations to Class Members that it was protecting this sensitive information.

9. Since the Data Breach, Class Members have been repeatedly harmed, and all of them are at risk for future identity theft given the loss of privacy of their Social Security numbers. Class members have spent countless hours filing police reports and poring over credit reports to combat identity theft, but new fraud is still being perpetrated against them using the sensitive information taken during the Data Breach. Many are now paying monthly or annual fees for identity theft and credit monitoring services that they trust, and others have had to place credit freezes on their accounts, which greatly hinders their ability to transact business and apply for credit as they could before the breach. Now that their sensitive personal information (e.g., their Social Security numbers, dates of birth, and home addresses) has been

released, Class Members must worry about being victimized throughout the rest of their lives.

10. Following the Data Breach, Defendant set up a website whereby consumers could enter in their last names and the last six digits of their Social Security numbers to determine if their PII has been compromised.

11. Consumers are then offered free enrollment in TrustedID Premier credit monitoring service for one year.

12. TrustedID is a credit monitoring service offered by Equifax. This service is inadequate to make Class Members whole. It lasts one year; yet, Class Members will be at risk for identity theft for the remainder of their lives, as some PII, such as a Social Security number, remains the same over the course of a consumer's lifetime.

13. In response to the Data Breach, Equifax's Chief Executive Officer, Richard Smith, Chief Information Officer, David Webb, and Chief Security Officer, Susan Mauldin, resigned their positions with the Company.

14. Because Defendant failed to provide even minimally adequate computer systems and data security practices, Class Members are forced to suffer the consequences. This Court must hold Defendant accountable.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class of Plaintiffs is a citizen of a state different from a Defendant.

16. This Court has personal jurisdiction over Defendant because Defendant has a principal place of business in Georgia and conducts business in the state of Georgia.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

PARTIES

A. Plaintiffs

18. Plaintiff Dianna Larson is a citizen and resident of the state of Michigan. Equifax collected her Personal Information, which Equifax maintained in its database. Ms. Larson learned that her PII was compromised in the Equifax data breach. On September 16, 2017, Ms. Larson received an alert from her credit monitoring service, creditsesame.com, that her credit card information was found on

the "Black Market." This was the first and thus far only time she was informed of this by creditsesame.com. Visa and MasterCard sent confidential alerts to financial institutions across the United States in mid-September, 2017, warning them that more than 200,000 credit cards were stolen in the Data Breach. As a result of the Data Breach, Ms. Larson has spent numerous hours addressing issues arising from the Data Breach.

19. Plaintiff Matthew Gates is a citizen and resident of the state of Florida. Equifax collected his Personal Information, which Equifax maintained in its database. Mr. Gates learned that his PII, and his son's PII, was compromised in the Equifax data breach when he logged onto the Equifax website, equifaxsecurity2017.com. As a result of the Data Breach, Mr. Gates has spent numerous hours addressing issues arising from the Data Breach.

20. Plaintiff, Christy Adams, is a citizen and resident of the Commonwealth of Pennsylvania. Equifax collected Ms. Adams's Personal Information, which Equifax maintained in its database. In 2011, Ms. Adams subscribed to Equifax's credit monitoring service "Equifax ID Patrol," providing Equifax with additional personal information and paying for that service continuously every month through the time that the Data Breach occurred. Ms. Adams was only alerted of the Data Breach through public media reports. Upon learning of the breach, Ms. Adams

checked the Equifax website to determine and confirm that her Personal Information may have been or was compromised as a result of the Data Breach. Upon visiting the website, Ms. Adams learned that "[b]ased on the information provided, we believe that your personal information may have been impacted by this incident." Ms. Adams must now engage in regular monitoring of her credit and bank accounts. As a result of the Data Breach, Ms. Adams has spent numerous hours signing up for credit monitoring and identity theft protection, and must continue to monitor her accounts with great vigilance to watch out for the presence of fraudulent charges or the creation of fraudulent new accounts.

21. Plaintiff, Gary Mares, is a citizen and resident of the State of California. Equifax collected Mr. Mares's Personal Information, which Equifax maintained in its database. Mr. Mares learned that his PII, and his wife's PII, was likely compromised in the Equifax data breach when he logged onto the Equifax website, equifaxsecurity2017.com. As a result of the Data Breach, Mr. Mares has spent numerous hours addressing issues arising from the Data Breach.

B. Defendant

22. Defendant Equifax, Inc. is incorporated and headquartered in Georgia. Defendant is one of the three major consumer credit reporting agencies in the United

States. Defendant operates through subsidiaries, including Equifax Information Services, LLC and Equifax Consumer Services, LLC.

CLASS ALLEGATIONS

23. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of FED. R. CIV. P. 23(a), 23(b)(2), and 23(b)(3) are met with respect to the Class defined below.

24. Plaintiffs bring this action as a national class action for themselves and all members of the following Class of similarly situated persons: All persons who reside in the United States whose PII was compromised as a result of the data breaches occurring at Equifax between March and August of 2017.

25. Excluded from the Class are Defendant, officers, directors, and employees of Defendant, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Court and its employees, officers, and relatives.

26. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

27. All members of the proposed Class are readily ascertainable, as Equifax has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

28. ***Numerosity.*** The Class is so numerous that joinder of all members is impracticable. Equifax announced 143 million consumers may be affected by the Data Breach. Accordingly, the Class likely includes many millions of members.

29. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the Class, including the following:

a) whether Defendant engaged in the wrongful conduct alleged in this Complaint;

b) whether Defendant's conduct was unlawful;

c) whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect Class Members' PII;

d) whether Defendant unlawfully used, maintained, lost, or disclosed Class members' PII;

e) whether Defendant unreasonably delayed in notifying affected customers of the security breach;

f) whether Defendant owed Plaintiffs and other Class Members a duty to exercise reasonable care in the keeping of their PII;

g) whether Defendant undertook a duty to safely store PII;

h) whether Plaintiffs and other Class Members were injured as a result;

i) whether Defendant knew or should have known that its computer systems were vulnerable to attack;

j) whether Plaintiffs and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

k) whether Defendant breached duties to Plaintiffs and the Class as a bailee of PII entrusted to it and for which Defendant owed a duty to safeguard and of safekeeping;

l) whether Plaintiffs and other Class Members are entitled to recover damages; and

m) whether Plaintiffs and other Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

30. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that the representative Plaintiffs, like all Class Members, had their PII compromised and stolen. Plaintiffs and all Class Members were injured through the uniform

misconduct of Defendants described in this Complaint and assert the same claims for relief.

31. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in class action and complex litigation, including in data breach litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of the Class.

32. ***Predominance.*** The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

33. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class. Plaintiffs and other Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation arising from the same data

breaches. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

34. Class certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

35. Class certification is appropriate under FED. R. CIV. P. 23(b)(2), in that Defendant has acted in a manner that applies generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate for the class.

COUNTS

COUNT I – VIOLATION OF GEORGIA'S UNIFORM DECEPTIVE TRADE PRACTICES ACT O.C.G.A. §10-1-370 *ET SEQ.*

36. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

37. Plaintiffs and Class Members are "persons" as defined by the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), O.C.G.A. §10-1-371(5).

38. Defendant violated and continues to violate the Georgia UDTPA by engaging in the unconscionable, deceptive, or unfair acts or practices as described herein. This conduct includes, inter alia, breaching duties Defendant owes to

Plaintiffs and the Class pursuant to O.C.G.A. §10-1-370, et seq., by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

39. By omitting the fact that Defendant could not provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII, it violated the Georgia UDTPA.

40. Plaintiffs and Class Members reasonably relied upon Defendant's omissions in turning over their PII to financial institutions and other entities that report PII to Defendant. Had Plaintiffs and other Class Members known Equifax would not secure their PII, they could have attempted prophylactic measures, such as placing credit freezes on their accounts or signing up for more extensive identity theft protection.

41. Defendant's omissions regarding its ability to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII was an act likely to mislead Plaintiffs and the members of the Class acting reasonably under the circumstances, and constitutes an unfair and deceptive trade practice in violation of the Georgia UDTPA.

42. Defendant knew or should have known that it had kept highly relevant and material information from consumers—namely information regarding its

inability to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII—and therefore violated the Georgia UDTPA.

43. As a direct and proximate result of Defendant's violation of the Georgia UDTPA, Plaintiffs and Class Members are at great risk going forward of experiencing identity theft.

44. Plaintiffs and the Class also seek equitable relief and to enjoin Defendant on the terms that the Court considers reasonable.

45. In addition, Plaintiffs and the Class seek reasonable attorneys' fees and costs incurred in bringing this action.

COUNT II – NEGLIGENCE

46. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

47. Defendant owed consumers a duty of reasonable care in the handling and safeguarding of their PII.

48. Defendant also had a duty to timely inform Plaintiffs and other Class Members that their PII been compromised or improperly furnished to unauthorized third parties.

49. Defendant, through the acts described herein, breached its duty of care by, *inter alia*,:

a) failing to properly implement and maintain adequate security measures to protect customer PII from being accessed, disseminated, or misused by unauthorized third parties;

b) failing to adequately store Plaintiffs' and other Class Members' PII; and

c) failing to timely and sufficiently notify Plaintiffs and other Class Members that their PII had been compromised or improperly accessed by unauthorized third parties.

50. As a direct and proximate result of Defendant's negligence, Plaintiffs and other Class Members have suffered, or will suffer, damages, including the costs associated with fraudulent purchases, identity theft, theft of funds, fees paid for credit freezes and other banking fees, fees paid for account freezes and stop payments, damage to credit scores, the cost of identity theft protection and/or credit monitoring services, and the diminution of the value of their PII, as they have lost the ability to control possession thereof.

COUNT III – NEGLIGENT PERFORMANCE OF AN UNDERTAKING

51. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

52. Financial institutions provided Defendant with Class Members' PII for the purposes of reporting payment history.

53. Equifax was aware that data security is necessary for the protection of Plaintiffs' and other Class Members' PII.

54. Financial institutions owed Plaintiffs and other Class Members a duty to adequately secure their PII.

55. Equifax failed to exercise reasonable care in providing data storage and security services for the protection of Plaintiffs' and other Class Members' PII, increasing the risk that their PII would be accessed and/or stolen by unauthorized third parties.

56. Plaintiffs and other Class Members relied upon whomever would be storing their PII to provide adequate security to protect their PII.

57. Upon turning over their PII, Plaintiffs and other Class Members lost any ability to control or protect their PII stored on Equifax's servers.

58. As a result of Defendant's negligence, Plaintiffs' and other Class Members' PII have been damaged. They have lost the ability to control who has possession of their property, thus diminishing its value.

59. As a result of this loss of control, Plaintiffs and other Class Members have been forced to expend resources to mitigate their losses and suffered damages arising from thieves' access to and usage of their PII.

COUNT IV – BAILMENT

60. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

61. Plaintiffs and Class Members submitted their PII to Defendant via various financial institutions.

62. PII constitutes a form of intangible personal property, as demonstrated, in part, by the resources and effort people expend to protect their PII and control who has possession thereof. Moreover, markets exist for both the lawful and unlawful transacting of PII.

63. Plaintiffs' and Class Members' property rights encompass the fundamental right to control who possesses their PII.

64. In delivering their PII, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their PII.

65. Defendant accepted possession of Plaintiffs' and Class Members' PII.

66. By accepting possession of Plaintiffs' and Class Members' PII, Defendant understood that Plaintiffs and other Class Members expected it to adequately safeguard their PII. Accordingly, a bailment was established for the mutual benefit of the parties.

67. Plaintiffs, other Class Members, and Defendant expected PII would be returned or otherwise duly accounted for at the end of the bailment.

68. Since PII is a form of intangible personal property, Plaintiffs' and other Class Members' exclusive possession can be restored by the deletion of their PII once financial institutions and other entities that purchase Credit Reports no longer need these data.[2]

69. During the bailment, Defendant owed a duty to Plaintiffs and other Class Members to exercise reasonable care, diligence, and prudence in protecting their PII and to maintain reasonable security procedures and practices to protect their PII.

70. Before the bailment relationship ended and prior to Defendant returning or duly accounting for Plaintiffs' and other Class Members' PII, Defendant breached this duty.

71. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and other Class Members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and other Class Members' PII.

[2] Another example of when Plaintiffs and other Class Members would expect Defendant to return or duly account for their PII would be if Equifax were to exit the consumer credit reporting business. Plaintiffs and other Class Members would not expect Defendant to retain possession of their PII in such a circumstance.

72. By failing to adequately secure Plaintiffs' and other Class Members' PII, Plaintiffs and other Class Members have lost exclusive possession of their PII and their ability to determine whom may possess their PII and for what purposes.

73. To date, Defendant has not returned or duly accounted for Plaintiffs' and other Class Members' PII. Because Plaintiffs' and other Class Members' PII remains available to thieves in a dispersed, worldwide network of computers, Defendant will not, at some future date, return or duly account for Plaintiffs' and other Class Members' PII.

74. As a result of Defendant's breach of bailment, Plaintiffs and other Class Members have suffered or will suffer damages, including the costs associated with fraudulent purchases, identity theft, theft of funds, fees paid for credit freezes, damage to credit scores, the cost of identity theft protection and/or credit monitoring services, and the diminution of the value of their PII as they have lost the ability to control possession thereof.

COUNT V – DECLARATORY JUDGMENT

75. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

76. Plaintiffs and Class Members have stated claims against Equifax based on negligence, negligent performance of an undertaking, breach of bailment, and violation of the Georgia UDTPA.

77. Defendant has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and Class Members, as indicated by the Data Breach that precipitated this lawsuit.

78. In addition, the Data Breach has rendered Defendant's system(s) even more vulnerable to unauthorized access and requires that Defendant immediately take even more stringent measures to currently safeguard the PII of Plaintiffs and Class Members going forward.

79. An actual controversy has arisen in the wake of Defendant's Data Breach regarding its current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Class.

80. Plaintiffs and Class Members thus seek a declaration that Defendant in not in compliance with its existing obligations, and that Defendant must implement specific additional, prudent security practices, as outlined below, to provide reasonable protection of Plaintiffs' and the Class Member's PII.

81. Specifically, Plaintiffs and the Class seek a declaration that Defendant must implement and maintain reasonable security measures on behalf of Plaintiffs

and the Class, including, but not limited to: (1) engaging third-party security auditors/penetration testers, as well as internal security personnel to conduct testing consistent with prudent data-security industry practices, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (2) engaging third-party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, PII not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store PII; and (8) meaningfully educating Data Breach victims about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

82. In addition, Plaintiffs and Class Members seek a declaration that to comply with its existing obligations, Defendant must provide credit monitoring and identity theft protection to Plaintiffs and Members of the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiffs to be Class representatives and their counsel to be Class counsel;

B. That the Court award Plaintiffs appropriate relief, to include actual and statutory damages, disgorgement, and restitution;

C. That the Court award Plaintiffs preliminary or other equitable or declaratory relief as may be appropriate by way of applicable law, including but not limited to the provision of credit and identity theft protection for the life of the victim;

D. That the Court enter such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations alleged herein;

E. That the Court award Plaintiffs such other, favorable relief as may be available and appropriate under law or at equity;

F. That the Court award costs and reasonable attorneys' fees; and

G. That the Court enter such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully submitted this 5th day of October, 2017.

Law Offices of David A. Bain, LLC

/s/ David A. Bain
David A. Bain
Georgia Bar No. 032449
1230 Peachtree Street, NE
Suite 1050
Atlanta, GA 30309
Tel: (404) 724-9990
Fax: (404) 724-9986
dbain@bain-law.com

Mark S. Goldman
Douglas J. Bench
GOLDMAN SCARLATO & PENNY, PC
Eight Tower Bridge, Ste. 1025
161 Washington Street
Conshohocken, PA 19428
Tel: (484) 342-0700
goldman@lawgsp.com
bench@lawgsp.com

Joshua H. Grabar
GRABAR LAW OFFICE
BNY Mellon Center
1735 Market Street
Suite 3750
Philadelphia, PA 19103
Tel: 267-507-6085
jgrabar@grabarlaw.com

Counsel for Plaintiffs and the Proposed Class